

AUSA LONG BEACH

28:MAY:2009



**C4, SPACE & CYBER: ENABLING THE
GLOBAL NETWORK ENTERPRISE CONSTRUCT**

LTC Jeff Sorenson

Chief Information Officer/G-6

**AMERICA'S ARMY: THE STRENGTH OF THE NATION
ARMY STRONG**



Agenda



- ④ **Restoring Balance**
- ④ **CONUS Based & Expeditionary**
- ④ **Global Network Enterprise Construct**
 - ◆ Network Service Centers
 - ◆ Operational Validation – AC09
- ④ **Cyber Operations & Warfare**
 - ◆ Army Cyber Operations & CND Support
 - ◆ USCYBERCOM & 7SC(T)
- ④ **C4 & Space**
- ④ **Conclusions**



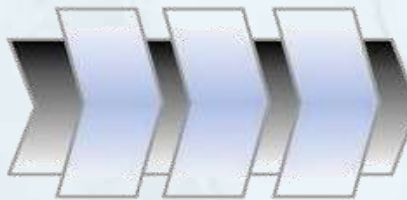
4 Army Imperatives

CURRENT



- Demand Exceeding Supply
- Dwell ~ 1:1 for AC & <1:4 for RC Soldiers
- Irregular Warfare-focused Force
- Limited Strategic Flexibility
- Accelerated Equipment Wear-Out
- Soldier and Family Stress

Restoring Balance



FUTURE



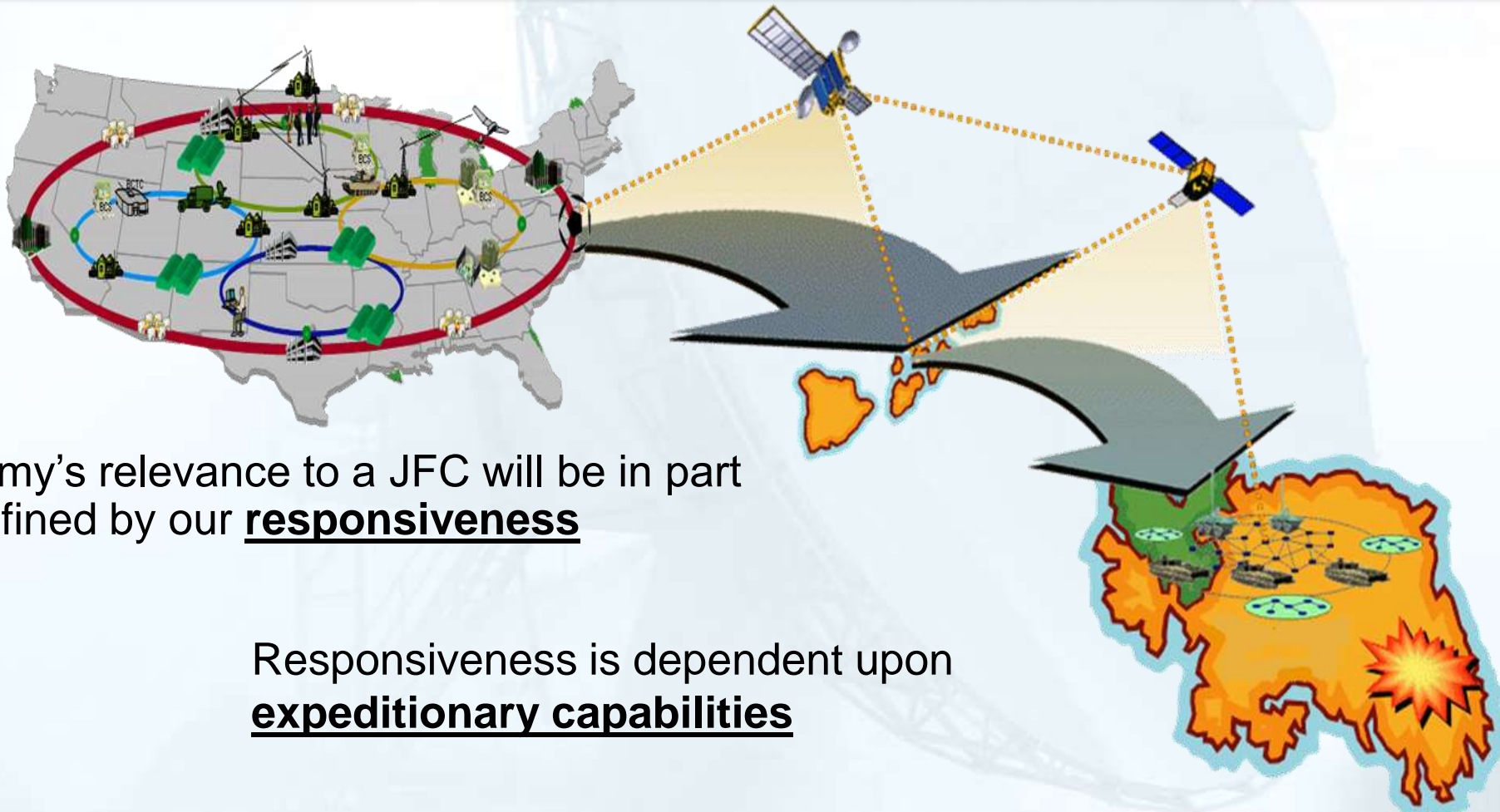
- Growth Completed
- Dwell ~ 1:2 for AC & ~ 1:4 for RC
- Base Realignment Complete
- Modular Reorganization Complete
- Rebalancing Complete
- Rotational Readiness Model Implemented
- Forces Ready for Full Spectrum of Operations

IMPERATIVES

- Sustain
- Prepare
- Reset
- Transform



Situation – CONUS Based and Expeditionary



Army's relevance to a JFC will be in part defined by our responsiveness

Responsiveness is dependent upon expeditionary capabilities

Many expeditionary capabilities are **NETWORK** dependent

- Transport



Strategic



Operational



Tactical

- Strategic fiber backbone links to tactical edge
- Enables pre-staging data and services for Expeditionary Modular Forces

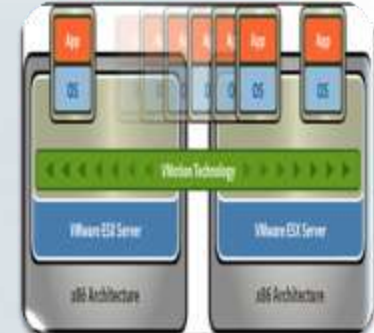
- Applications



Strategic



Operational



Tactical

- Strategic computing centers provide storage and processors
- Enables pre-staging data and services for Expeditionary Modular Forces

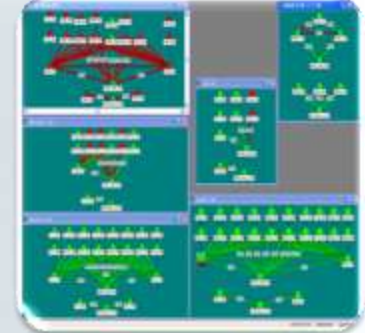
- NetOps



Strategic



Operational



Tactical

- NetOps coordinates elements required to maneuver data and services in support of the Main Effort
- Understand, Visualize, Describe, and Direct the Network



Network Service Center – Concept



Regional Hub Node (RHN)

- Provides Global Transport
- Intra-Theater Connectivity
- Up to 3 Div per Hub Node
- Connect to each other & DISN services in garrison

Area Processing Center (APC)

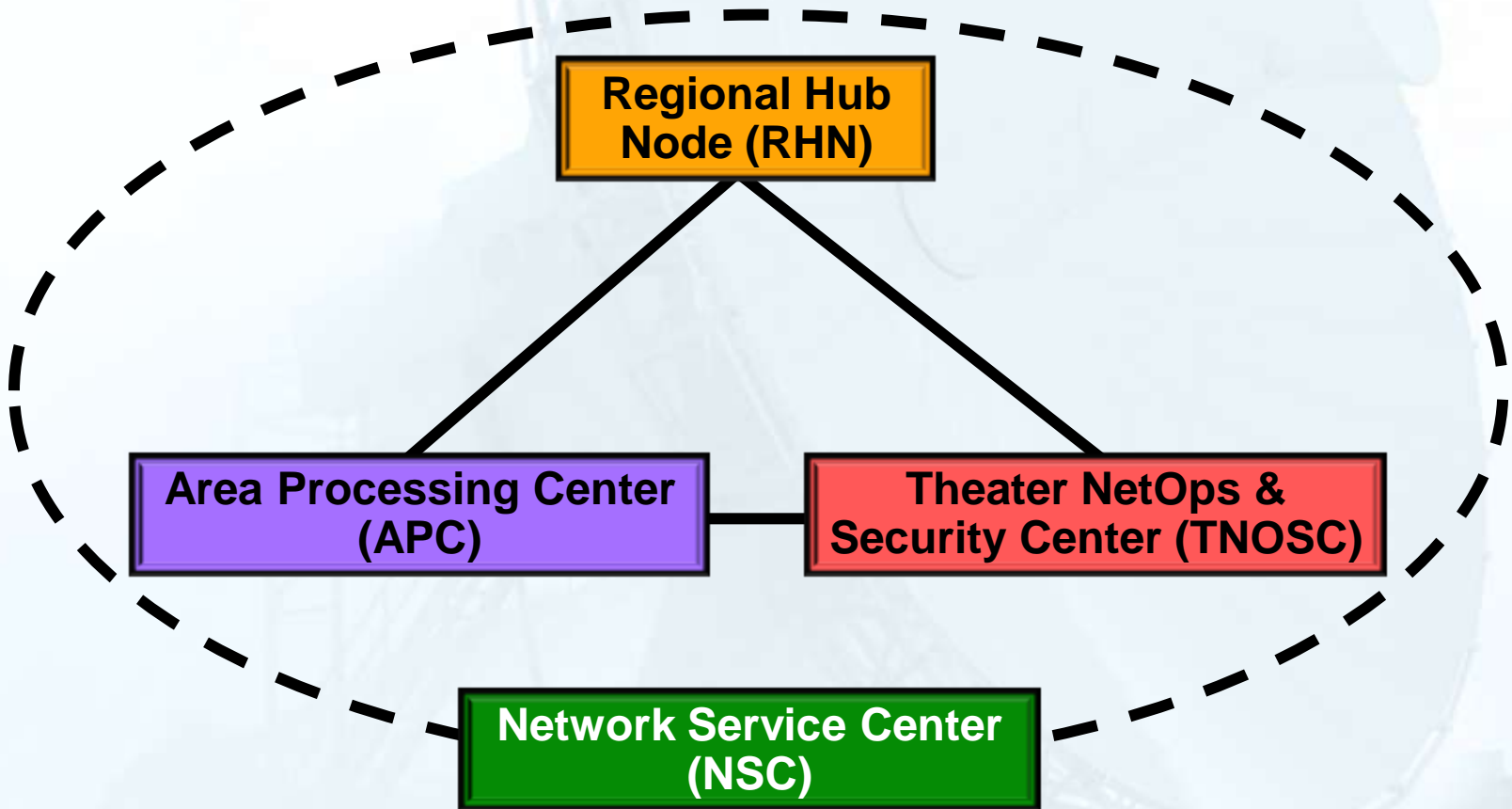
- Data & Applications
- Consolidated IT hardware
- Projection & forward staging of info & services

Theater NetOps & Security Center (TNOSC)

- Technical oversight, enterprise, content, spectrum & Help Desk
- NetOps SA & optimize GIG avail
- Information Assurance & Security



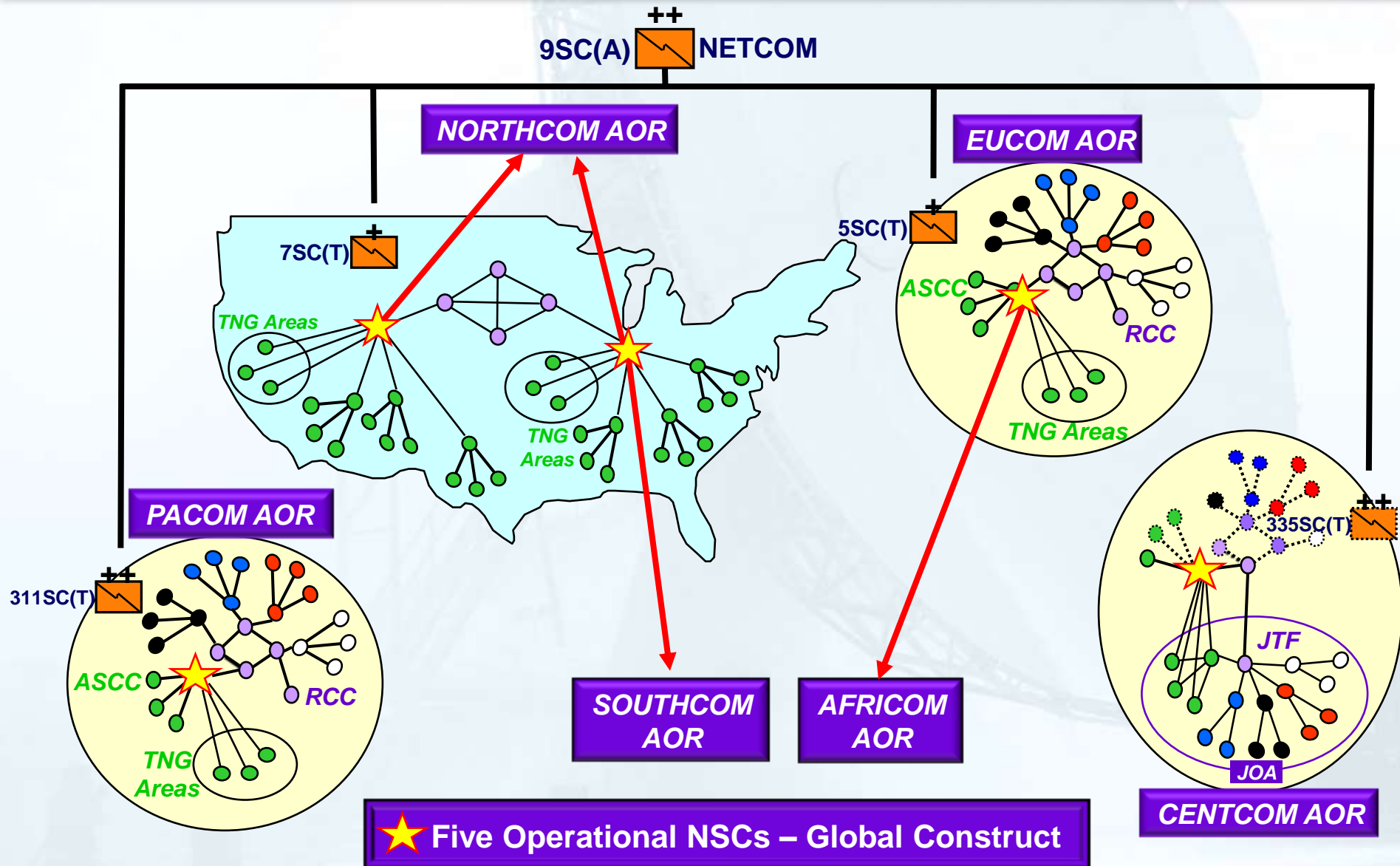
Network Service Center – Concept



The “Always On” Network



Global NSC Construct

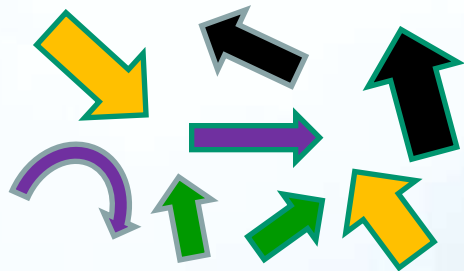




NSC Concept of Operation

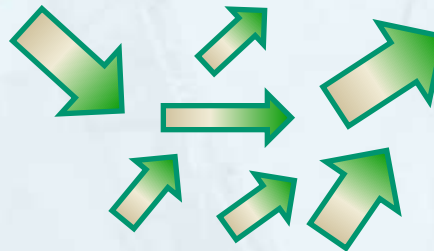


\$\$\$\$\$



Organizational

\$\$\$\$



Federated

\$\$\$



Enterprise

LandWarNet Now

- Fragmented
- Not Standardized
- Unsecure
- Expensive

Operating Principles



LandWarNet Future

- Global
- Standardized
- Protected
- Economical



CSA – GNEC Memo



- “transforming to become...a versatile, expeditionary force capable of full-spectrum operations”
- “synchronize...with other Army activities...ARFORGEN, BRAC, GDP”
- “We will use the...GNEC as the network enterprise strategy”
- “CIO/G6 will establish new procedures to **operationalize** ... improve the overall **security** ... achieve better **efficiencies** ... pursue joint **interoperability** as we construct our network enterprise”
- “all Army generating force networks will be managed by a single command (NETCOM) organizing Army information to make it globally accessible, useful and secure for soldiers deployed anywhere”



UNITED STATES ARMY
THE CHIEF OF STAFF

MAR 2 2008

MEMORANDUM FOR SEE DISTRIBUTION


SUBJECT: LandWarNet – Global Network Enterprise Construct Strategy Implementation

1. We are transforming to become a fundamentally different Army—a versatile, expeditionary force capable of full-spectrum operations. To support this Army, we must fundamentally change and adapt our institutions, including LandWarNet—the Army's portion of the Global Information Grid. Over the next three years, the Army will transform LandWarNet to a centralized, more secure, operationalized, and sustainable network capable of supporting an expeditionary Army in this era of persistent conflict. To lay the foundation for further network expansion in the future, we will synchronize this transformation with other Army activities including the Army Force Generation model, Base Realignment and Closure, and Global Defense Posture Realignment. In FY09, we will set the foundation for the global network by achieving an initial operating capability of a network service center (NSC) in Europe; expanding these NSCs throughout all other Theaters by FY11.

2. We will use the Global Network Enterprise Construct (GNEC) as the network enterprise strategy. The CIO/G6 will establish new procedures to operationalize the network and improve the overall security of network services and capabilities. We will modify purchasing procedures to achieve better efficiencies in the procurement of our IT systems, and we will pursue joint interoperability with our other Service partners as we construct our network enterprise.

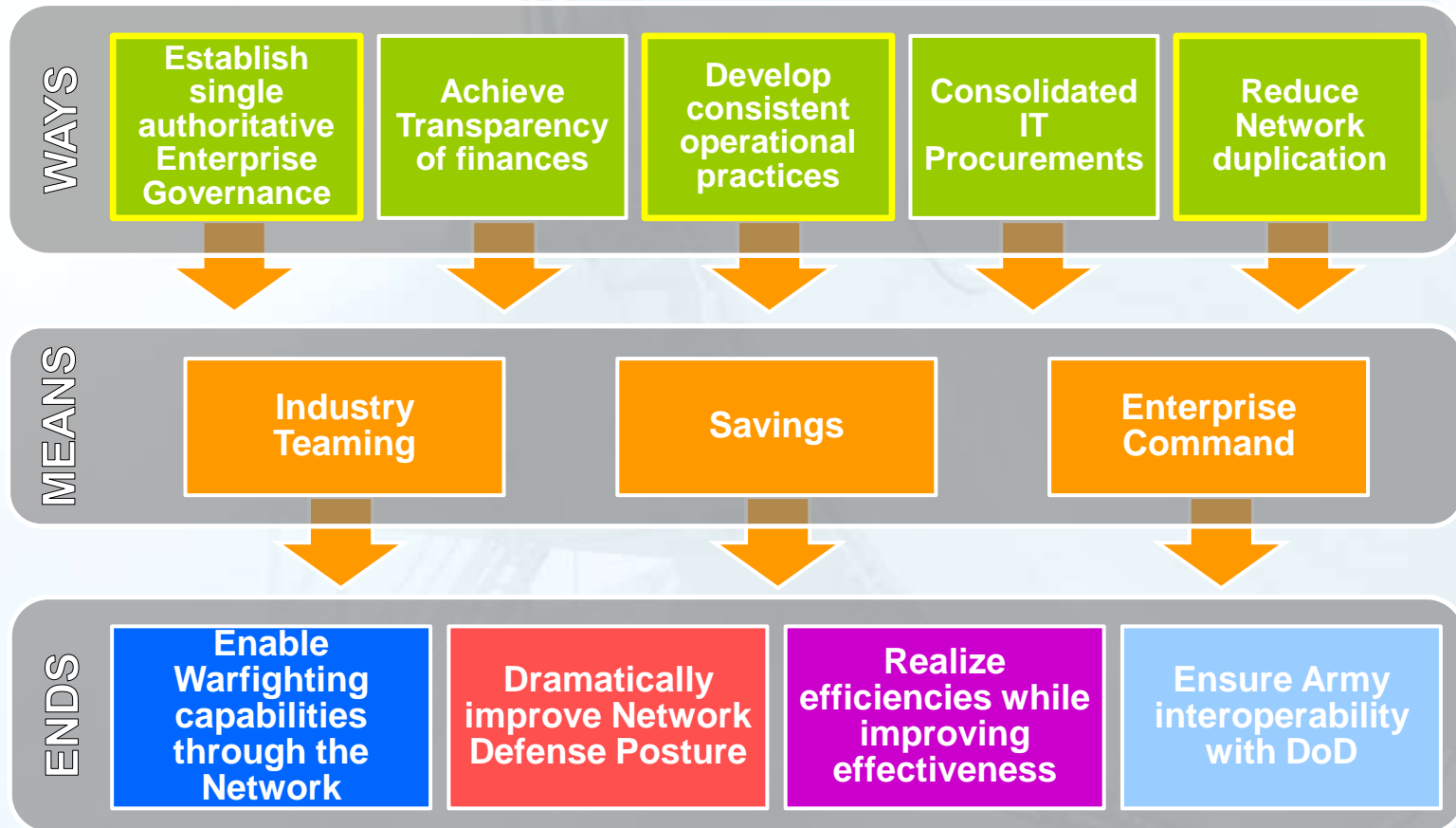
3. In the end, all Army generating force networks will be managed by a single command (Network Enterprise Technology Command (NETCOM)) organizing Army information to make it globally accessible, useful and secure for Soldiers deployed anywhere in the world.

4. The establishment of the Army global network enterprise requires dramatic changes to our current processes and network operations. Our combat-seasoned force is the best in the world, and transforming our network enterprise is central to a land force capable of conducting full-spectrum operations in the 21st Century. Your support is essential for our success.


GEORGE W. CASEY, JR.
General, United States Army



Strategy



Transition from multiple unit-owned networks to single enterprise network



Implementation Strategy



Phase 1: FY09 – NSC in Europe

- Aggregate/Discover & Establish Network – Main effort: CONUS, Europe & SWA; Supporting: PAC
- Focus on greater collaboration & network access to lower echelons, eliminate expeditionary capability gaps to CONUS & Europe
- Enhance ability to provide and defend Network & Governance

Phase 2: FY10 – NSCs in CONUS & SWA

- Extend Network – Main effort: CONUS, Europe & SWA; Supporting: PAC
- Eliminate more expeditionary capability gaps CONUS, Europe & SWA

Phase 3: FY11 and Beyond – NSC in Pacific

- Complete Network – Main effort: PAC; Supporting: CONUS, Europe & SWA
- Ubiquitous access – globally consistent security policies

Theater-based NSC deployment with Global effectiveness & efficiencies improvements

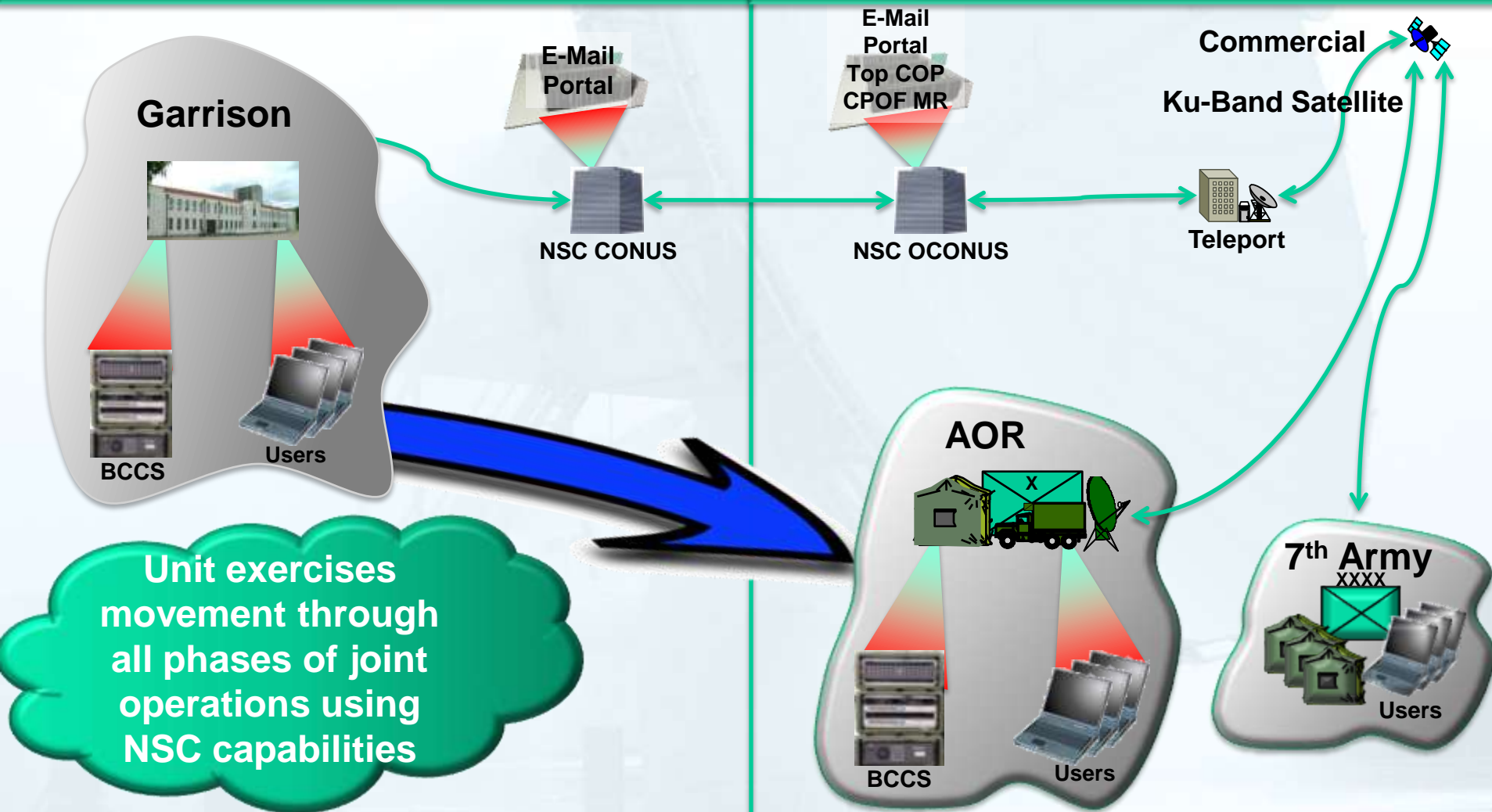


GNEC OPVAL Concept



CONUS

OCONUS





Objectives

Operational

- Seamlessly transition BCT from CONUS-OCONUS
- NSC Handoff between two Signal Command (Theater)
- Continuity of Operations selected Battle Command
- Refine NSC Doctrine
- Demo Battle Command application delivery from the Enterprise

Technical

- SIPRNet Collaboration build-out at two APCs
- Demo Single Identity
- Validate Resource Forest for Collaboration
- Satellite cross-strapping in support of operations

Training

- NSC Concept of Ops & Tactics, Techniques & Procedures (TTP)
- CONUS/Europe multi-Theater Signal Ops
- Refine Battle Command Assistance Team (BCAT)
- Exercise NETCOM Staff under GNEC
- Exercise early cross-theater collaboration



GNEC OPVAL Demo – AC 09



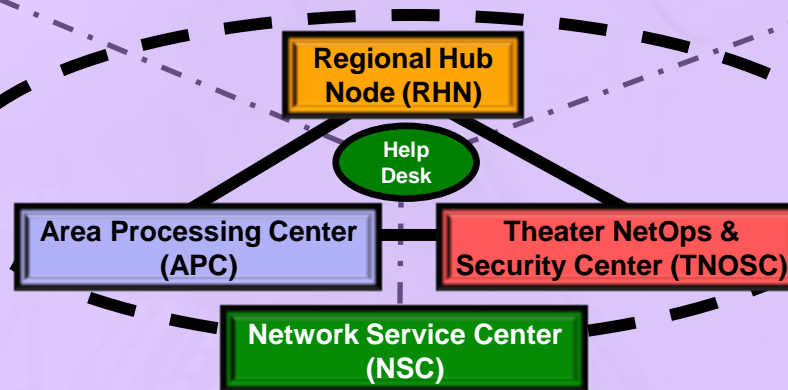
RED = Demonstrated in AC 09

Connectivity

- **GIG Integration**
- **Regional Networks**
- **Base Infrastructure**
- **SATCOM Connect/Management**
- **DISN Optimization**
- **Single DOIM**

Services

- **Data Strategy**
- **Authoritative Data**
- **Data Warehouse**
- **Virtualized Services**
- **Web Portals**
- **SOA**
- **Collaboration**
- **Integration of Joint Services**
- **Portfolio Management**
- **Green IT**



Other

- **Global/Theater Commands**
- **Joint Basing Communications**
- **Enterprise Governance**
- **Network Training**

NetOps

- **Security Policy**
- **Service Level Agreements**
- **Global Identity Mgmt**
- **Single Logical Network/Federation**
- **Network Provisioning**
- **Network SA**
- **Content Delivery/Caching**
- **Spectrum Mgmt**

Global Network Enterprise Construct (GNEC)



AC 09 OPVAL – Accomplishments



➤ Operational:

- ◆ Completed ROC Drills with NSC CONOPS, Control Plan & detailed script
- ◆ Employment of first 7SC(T) Network Enterprise Support Team (NEST)
- ◆ Executed Phases 0/1 (WARNORD) & 2/3 (BCCS Bragg→Grafenwöhr APC)
- ◆ 18th Fires Bde provided Battle Command services & standard services

➤ Technical:

- ◆ Build out 2 SIPRNet APCs (Ft Bragg & Grafenwöhr GE)
- ◆ PEO C3T field & train new Battle Command suite (BCCSv3) to 18th Fires Bde
- ◆ Virtualized 18th Fires Bde BCCSv3 within SIPRNet APCs
- ◆ Satellite cross-strap between 18th Fires Bde JNN and Germany RHN

➤ Training:

- ◆ Finalized 10 specific NSC Tactics, Techniques & Procedures (TTP)
- ◆ Trained 20+ Observer-Controllers (OC) to validate OPVAL Measures of Effectiveness/Performance (MoE/MoP)
- ◆ OC evaluation of OPVAL Phases 0-3
- ◆ 18th Fires Bde operating BCCSv3 & standard services virtually via remote RHN connection



Timeline



CSA Memorandum:

LWN-GNEC Implementation (2 Mar 09)

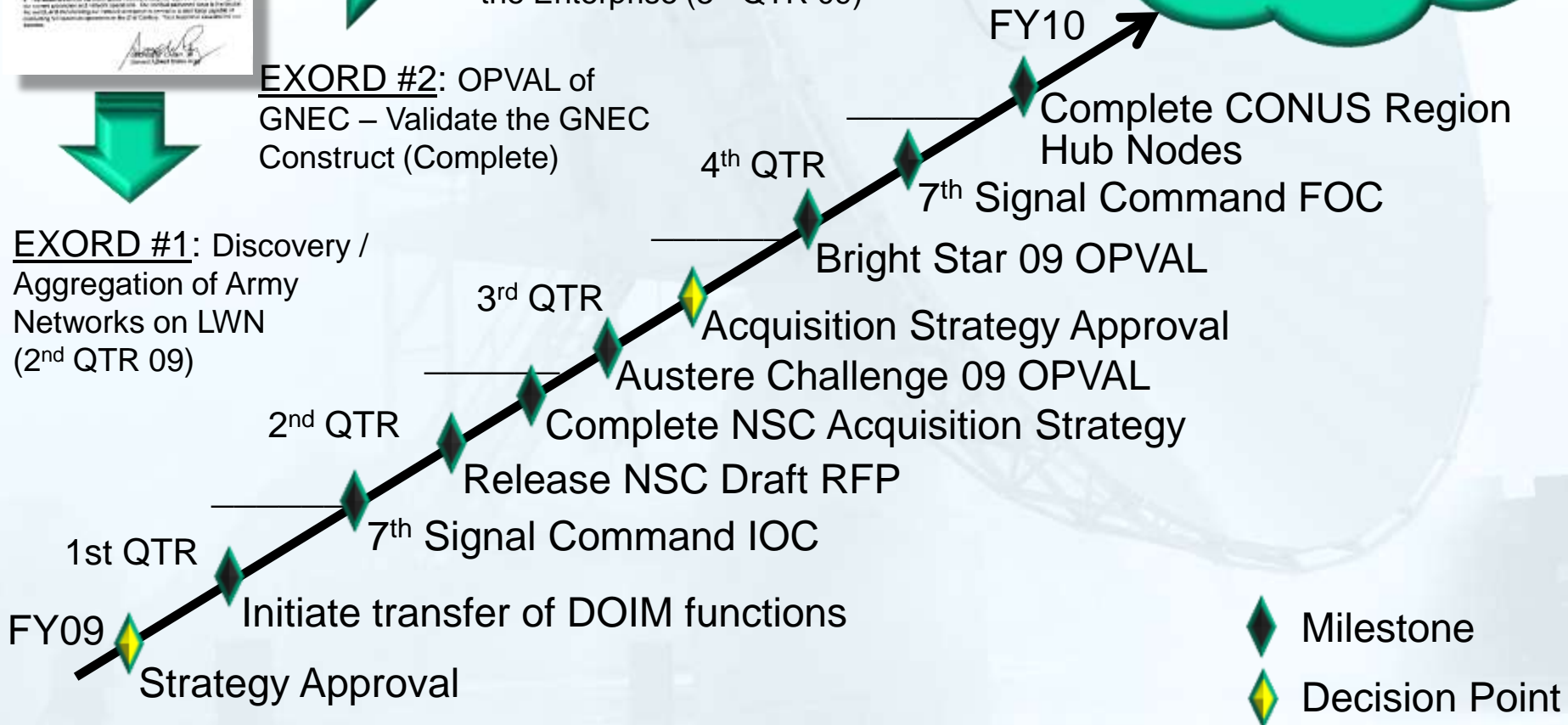


EXORD #3: Transformation of Installation Network Functions to the Enterprise (3rd QTR 09)

EXORD #2: OPVAL of GNEC – Validate the GNEC Construct (Complete)



EXORD #1: Discovery / Aggregation of Army Networks on LWN (2nd QTR 09)





Cyber Operations Governance



General Kevin P. Chilton
CDR USSTRATCOM



LTG Pollett
CDR JTF-GNO
BG Davis
DEP CDR JTF-GNO

Headquarters (4)



OSD (x2)



DOD IG



Joint Staff

Services (4)



Army



Air Force



Navy



Marine Corps

NetOps Ctrs (7)



DISA (x7)

Operational Control of Service
Network Operations and Security Centers

Combatant Commanders (10)



SOCOM



CENTCOM



EUCOM



PACOM



SOUTHCAM



STRATCOM



NORTHCOM



JFCOM



TRANSCOM



AFRICOM

Agencies
Field Activities
Others (40)



Network Defense Definitions



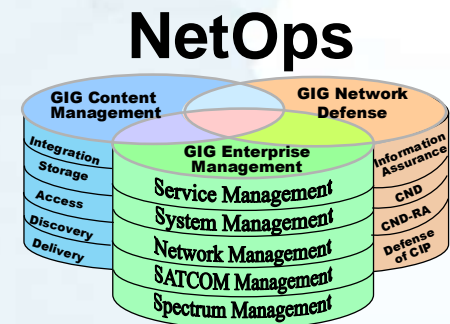
Network Defense: Incorporates end-to-end protection, detection, and response to unauthorized access, inadvertent damage, or modification of data and the GIG (JP 6-0)

Information Assurance: Measures to insure availability, integrity, authentication, confidentiality, non-repudiation, and restoration of information and systems (FM 3-0, JP 3-13)

Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and networks (FM 3-0, JP 6-0)

Computer Network Defense – Response Actions (CND-RA):
Defensive measures or activities to protect and defend DoD computer systems and networks under attack (GIG NetOps CONOPS)

Critical Infrastructure Protection (CIP): Actions to prevent, remediate, or mitigate risks resulting from vulnerabilities of critical infrastructure assets (JP 1-02, JP 6-0)



Network Defense:
IA
CND
CND-RA
CIP



Information Assurance vs. CND



➤ Information Assurance (IA)

- ◆ Measures to insure availability, integrity, authentication, confidentiality, non-repudiation, and restoration of information and systems
- ◆ Considers both technical and non-technical information protection measures (such as risk management, personnel training, audits, business continuity/disaster recovery planning, etc.)
- ◆ Holistically factors all incidents that occur through malicious or non-malicious activity by enemy or friendly entities

➤ Computer Network Defense (CND)

- ◆ Operational component of IA – provides defensive measures to protect and defend information, information systems, and networks from disruption, denial, degradation, or destruction
- ◆ Established to achieve technical actions of IA performed specifically to protect, monitor, analyze, detect, and respond to unauthorized, malicious activity on Army networks



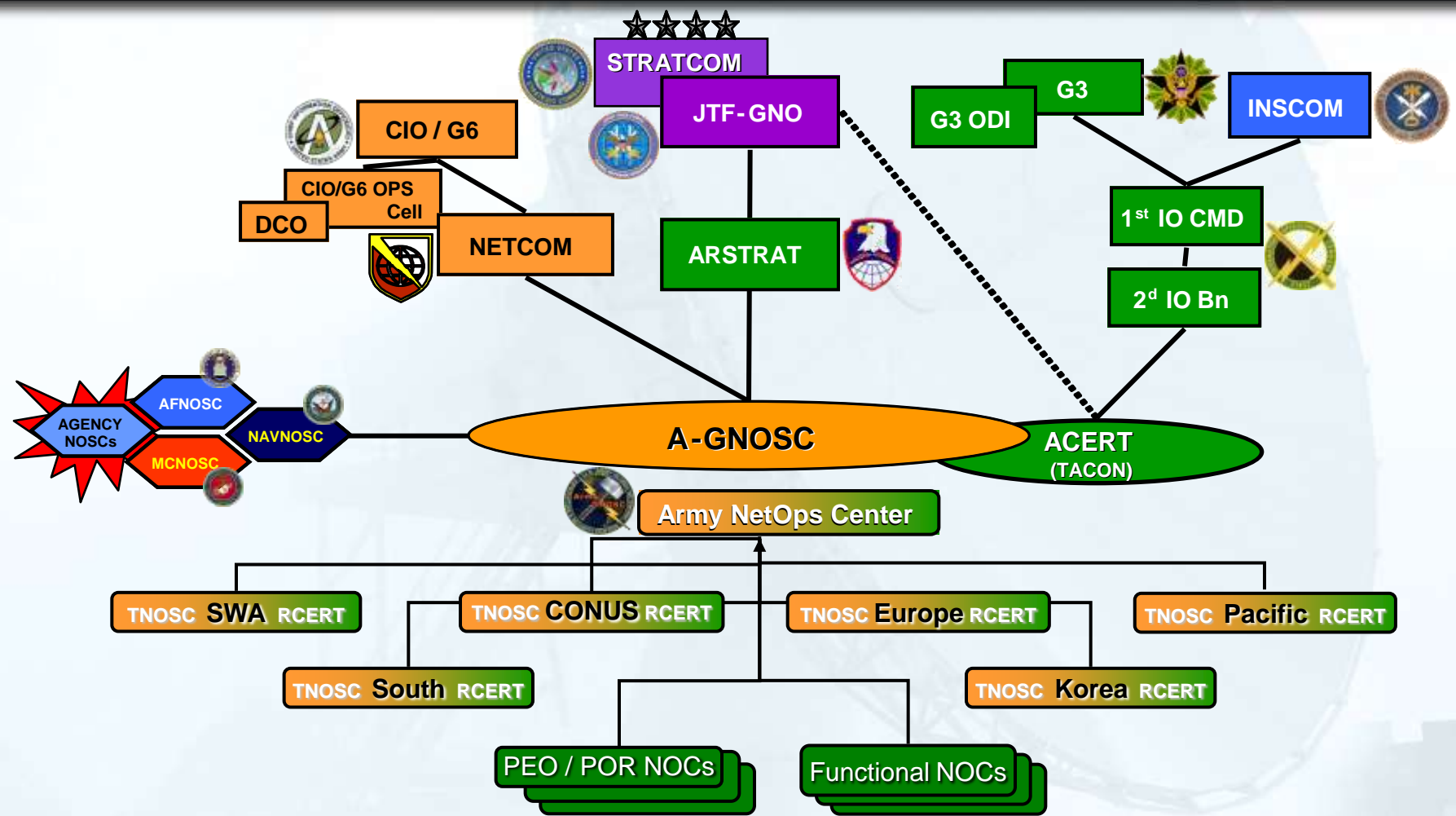
Warfighter Requirements



- Ability to gain situational awareness/understanding of operations in Army cyberspace
- Ability to conduct operations that ensure units can freely establish and access Army cyberspace
- Ability to command and control warfighting functions in Army cyberspace
- Ability to conduct an intelligence preparation of the operational cyber-environment
- Ability to protect information and information systems from harm
- Ability to sustain Army cyberspace in order to achieve mission assurance
- Ability to direct the movement and maneuver of information within Army cyberspace
- Ability for the commander to deliver net-enabled effects in and through Army cyberspace



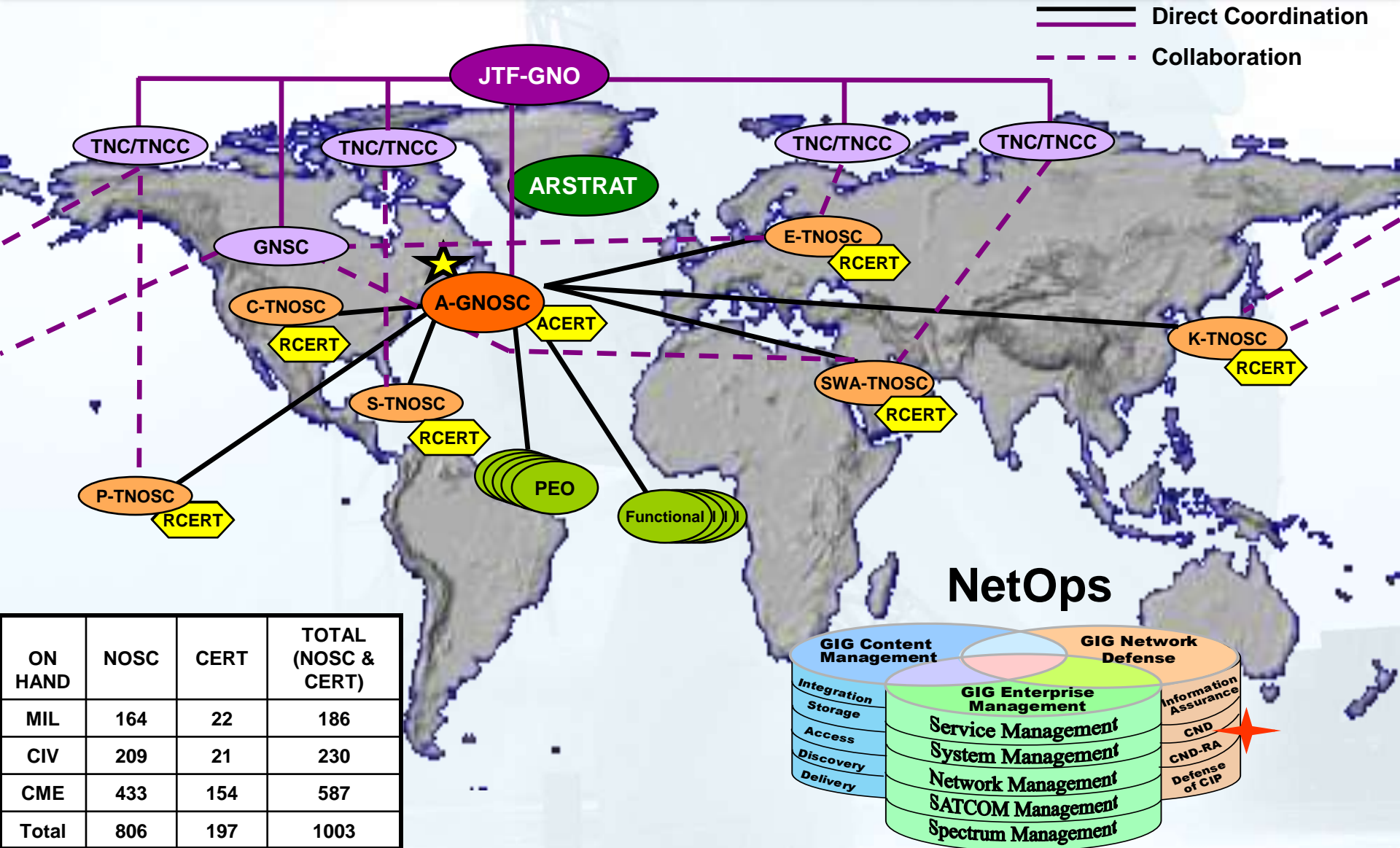
Army Cyber Operations Support



CNE/CNA 350	CNO/SIGINT 288	NetOps/CND 1,003
* Excluding Tactical Forces		
Current Total 1,641 Cyber Soldiers*		



Army CND Service Providers





“Strategy to Task” for Cyberspace



US Government/DoD/Joint

National Strategy to Defend Cyberspace

National Security Presidential Dir 54 – Cybersecurity Policy

DHS Comprehensive National Cybersecurity Initiative

National Military Strategy for Cyberspace Operations (NMS-CO)

NMS-CO Cyberspace Implementation Plan

Unified Command Plan (UCP) – 2008

USSTRATCOM Concept Plan 8039

USSTRATCOM Operational Concept for Cyberspace

USSTRATCOM Cyber DOTMLPF Change Request

USSTRATCOM Joint Manning Document – Joint Functional Component Command – Network Warfare

Joint Staff Action Processing Form 08-01907 – Cyberspace Operations Definition

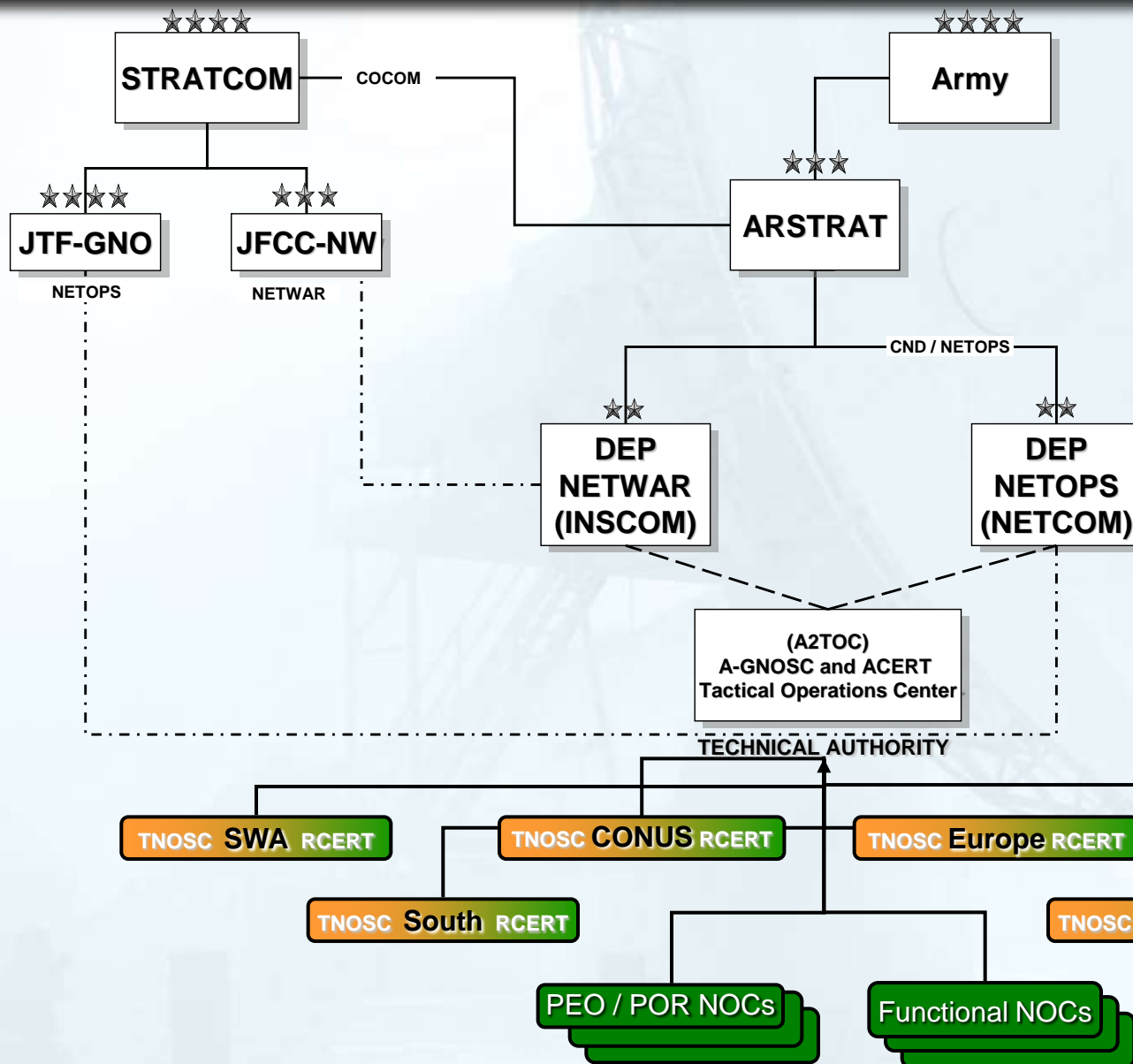
Joint Staff Action Processing Form 08-00559 – Proposed US Cyber Command

Army

- Computer Network Operations Standing Execute Order 096-08
- Army Provisional Network Warfare Battalion
- Army Operations Plan 8039
- Army Cyber Career Field Model (in development)
- Staffing formal Army response to OSD/QDR questions and Army position for recommended DoD cyber organization



Army Cyber Command & Control (C2)



- Department of the Army Execute Order defines Army C2 relationships for CNO
- Army "Cyber" forces are completely integrated (National to Tactical)
- INSCOM, NETCOM, and 1st Information Operations Command maintain global presence
- The Army is formidable in cyberspace; and growing to keep pace with the enemy



VCSA – ACTF ALARACT



UNCLASSIFIED//

THIS MESSAGE HAS BEEN SENT BY THE PENTAGON TELECOMMUNICATIONS CENTER ON BEHALF OF DA WASHINGTON DC//DAMO-OD ON BEHALF OF VICE CHIEF OF STAFF, ARMY//

SUBJ: ACTIVATION OF US ARMY CYBERSPACE TASK FORCE (ACTF)

REF A/MSGID: MSGHQDA/251855Z JAN 08

REF B/MSGID: MEMO/CYBERSPACE DEFINITION/12 MAY 2008

REF C/MSGID: MEMO/CYBERSPACE OPERATIONS DEFINITION/15 OCT 2008

REF D/MSGID: MEETING AMONG DCS G-2, DCS G-3/5/7, AND CIO/G-6/30 MAR 2009

REF E/MSGID: DODD 3600.01/INFORMATION OPERATIONS/14 AUG 2008

REF A IS THE HQDA EXORD WHICH DESCRIBES HOW COMPUTER NETWORK OPERATIONS IS EXERCISED IN THE ARMY.

REF B IS THE DEPSECDEF DEFINITION OF CYBERSPACE.

REF C IS THE DEPSECDEF DEFINITION OF CYBERSPACE OPERATIONS.

REF D IS THE DCS G-2, DCS G-3/5/7, CIO/G-6 AGREEMENT TO ESTABLISH AN ARMY CYBERSPACE OPERATIONS TASK FORCE.

REF E IS THE DOD DIRECTIVE THAT DEFINES THE TERM INFORMATION OPERATIONS.

NARR(U). THIS IS THE HQDA ACTIVATION OF THE ARMY CYBERSPACE TASK FORCE.

1. THIS MESSAGE ANNOUNCES THE ESTABLISHMENT OF THE US ARMY CYBERSPACE TASK FORCE (ACTF) AND OUTLINES ITS MISSION AND FUNCTIONS. THIS MESSAGE ALSO INCLUDES THE RESPONSIBILITIES FOR INTEGRATING CYBERSPACE ISSUES WITHIN THE ARMY STAFF (ARSTAF).

2. THE ARMY G-3/5/7 IS DIRECTED TO ESTABLISH THE ACTF WHICH WILL RESIDE WITHIN THE DIRECTORATE OF OPERATIONS, READINESS AND MOBILIZATION (DAMO-OD/G-33).

3. MISSION: THE MISSION OF THE ACTF IS TO INTEGRATE EFFORTS ACROSS THE ARSTAF TO PROVIDE POLICY, OVERSIGHT, AND GUIDANCE FOR ARMY CYBERSPACE AND CYBERSPACE OPERATIONS.

4. CONCEPT OF OPERATION: THE ACTF WILL DEVELOP AND INSTITUTIONALIZE POLICY, PROCEDURES, AND VALIDATE REQUIREMENTS AND PROVIDE RESOURCES FOR ADVANCED TECHNOLOGICAL SOLUTIONS DESIGNED TO ENABLE ARMY'S ABILITY TO OPERATE IN CYBERSPACE FROM THE STRATEGIC THROUGH TACTICAL LEVELS OF WARFARE. THE ACTF WILL MODIFY THE COMPUTER NETWORK OPERATIONS (CNO) EXORD WITHIN 60 DAYS OF ACTIVATION. THE EXORD WILL CLARIFY ARMY AUTHORITIES, ROLES, FUNCTIONS, SUPPORT AND COMMAND AND CONTROL RELATIONSHIPS FOR ARMY CYBERSPACE ORGANIZATIONS AND CYBERSPACE OPERATIONS.

5. TASK ORGANIZATION: CYBERSPACE OPERATIONS CROSSES NUMEROUS RESPONSIBILITIES AND FUNCTIONS WHICH REQUIRES THE ACTF MEMBERSHIP TO CONSIST OF REPRESENTATION FROM THE DCS G-2, DCS G-3/5/7, AND CHIEF INFORMATION OFFICER/G-6. EACH RESPECTIVE STAFF WILL PROVIDE PERSONNEL TO THE TASK FORCE, SERVING UNDER THE G-33, TO ENSURE CONTINUITY OF EFFORT.

6. DECONFLICTION: COMPUTER NETWORK OPERATIONS IS A COMPONENT OF BOTH CYBERSPACE OPERATIONS AND INFORMATION OPERATIONS AND REQUIRES DECONFLICTION AT THE NATIONAL AND JOINT LEVELS. THE HQDA ACTF WILL COORDINATE ALL CNO RELATED ACTIONS IN ACCORDANCE WITH REF A AND THE TO BE PUBLISHED EXORD IN ACCORDANCE WITH NATIONAL, DOD AND JOINT GUIDANCE.

7. THIS MESSAGE WILL REMAIN IN EFFECT UNTIL RESCINDED.

8. POC FOR THIS ACTION IS LTC BRYANT GLANDO, G-3/5/7, DAMO-ODI, AT COMMERCIAL: (703) 697-3637.

9. EXPIRATION DATE CANNOT BE DETERMINED TOP OF MESSAGE

- “Announces establishment of the US Army Cyberspace Task Force (ACTF) and outlines its missions and functions”
- “Army G-3/5/7 is directed to establish the ACTF which will reside within the Directorate of Operations, Readiness and Mobilization”
- “Mission of the ACTF is to integrate efforts across the ARSTAF to provide policy, oversight, and guidance for Army Cyberspace and Cyberspace operations”
- “ACTF membership to consist of representation from the DCS G-2, G-3/5/7, and CIO/G-6 ... serving under the G-33”
- “CNO is a component of both Cyberspace Operations and Information Operations and requires deconfliction at the National and Joint levels”



Challenges



- Vulnerability of critical infrastructures
 - ◆ Banking, Finance, etc.
 - ◆ Impact on military operations
- Adversaries are well trained and equipped
- Users are our greatest vulnerability...they are attacked 24/7
- Risks posed by foreign interests/ownership of tools we purchase
- Need for cyber professionals
 - ◆ Deep technical skills that cross all cyber elements
 - ◆ Understand how to incorporate cyber operations into the deliberate planning process










CND Support Examples



Long Range Plan

Mid-Range Plan

 ARMY CIO / G6	 NETCOM	 A-GNOSC	 ACERT / 1ST IO
<ul style="list-style-type: none">– Policy– CIO / EB– Portfolio Mgmt– NetOps Campaign Plan	<ul style="list-style-type: none">– Capabilities Design– CONOPS development– Test Plan– Pilot– Implementation Plan	<ul style="list-style-type: none">– IA Vulnerability Message Mgmt– IP Block– Global NetOps Directives– SA Formula, NetCrop Portal	<ul style="list-style-type: none">– Detailed Media Analysis– Enterprise Sensor Management– Global Security Event Correlation
 SIG Center TRADOC	<ul style="list-style-type: none">– Initial Funding– LOM	<ul style="list-style-type: none">– DNS Poisoning– POR Integration	<ul style="list-style-type: none">– Malicious Code Behavioral Analysis– Collection Plan
<ul style="list-style-type: none">– Doctrine– Training Development– Force Integration– Mobilization	<div><div data-bbox="836 739 884 1110">E P E</div><ul style="list-style-type: none">– New Equipment Training<hr/><div data-bbox="836 1153 884 1325">O I A C</div><ul style="list-style-type: none">– Controller IA Funding– Guidance IA Policy– Initial CON / ATO</div>	<ul style="list-style-type: none">– Enterprise Tools Mgmt– Vulnerability Mgmt– CNO Integration– TTPs– Battle Command Assistance Team (BCAT)– Remediation Lead	<ul style="list-style-type: none">– Technical Assessment– Forensic Malware Analysis– Vulnerability Assessment Team– Technical Support Analysis



Enduring CND Capabilities



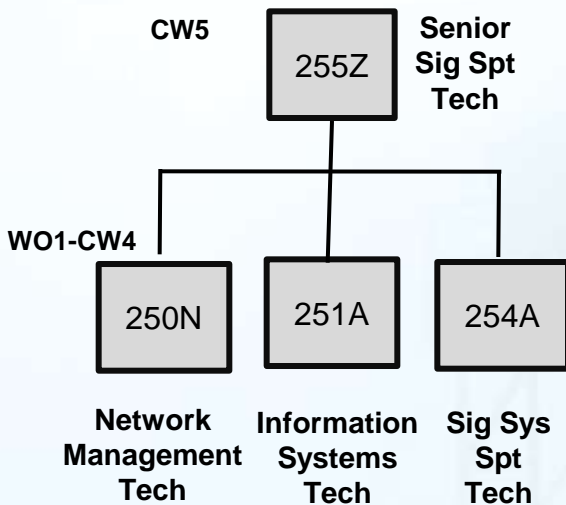
- **Protect** Army information, information systems, and communications networks from unauthorized, malicious activity
- **Monitor** Army information, information systems, and communications networks for unauthorized, malicious activity
- **Detect** unauthorized, malicious activity within Army information, information systems, and communications networks
- **Analyze** unauthorized, malicious activity within Army information, information systems, and communications networks
- **Respond** to unauthorized, malicious activity within Army information, information systems, and communications networks



Summary of Signal Warrant Officer Realignment



Current MOS Structure FY08



Merge into New MOS 255A

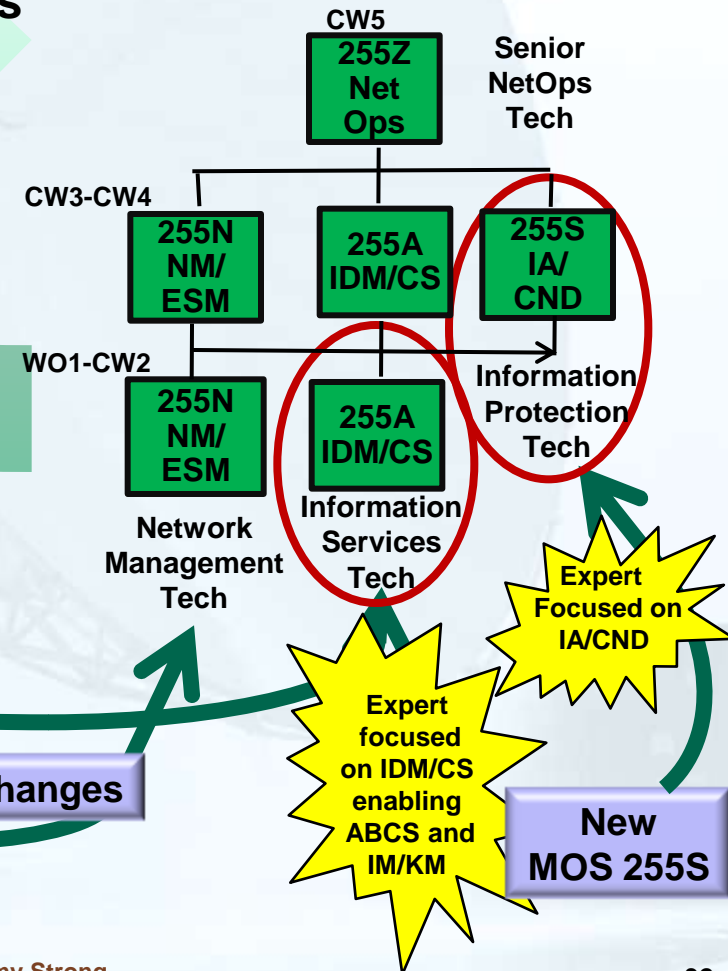
New MOS 255N w/minor changes

Cyber NetOps Functions

- NM/ESM
- IDM/CS (+ VI)
- IA/CND (+ EMSO)

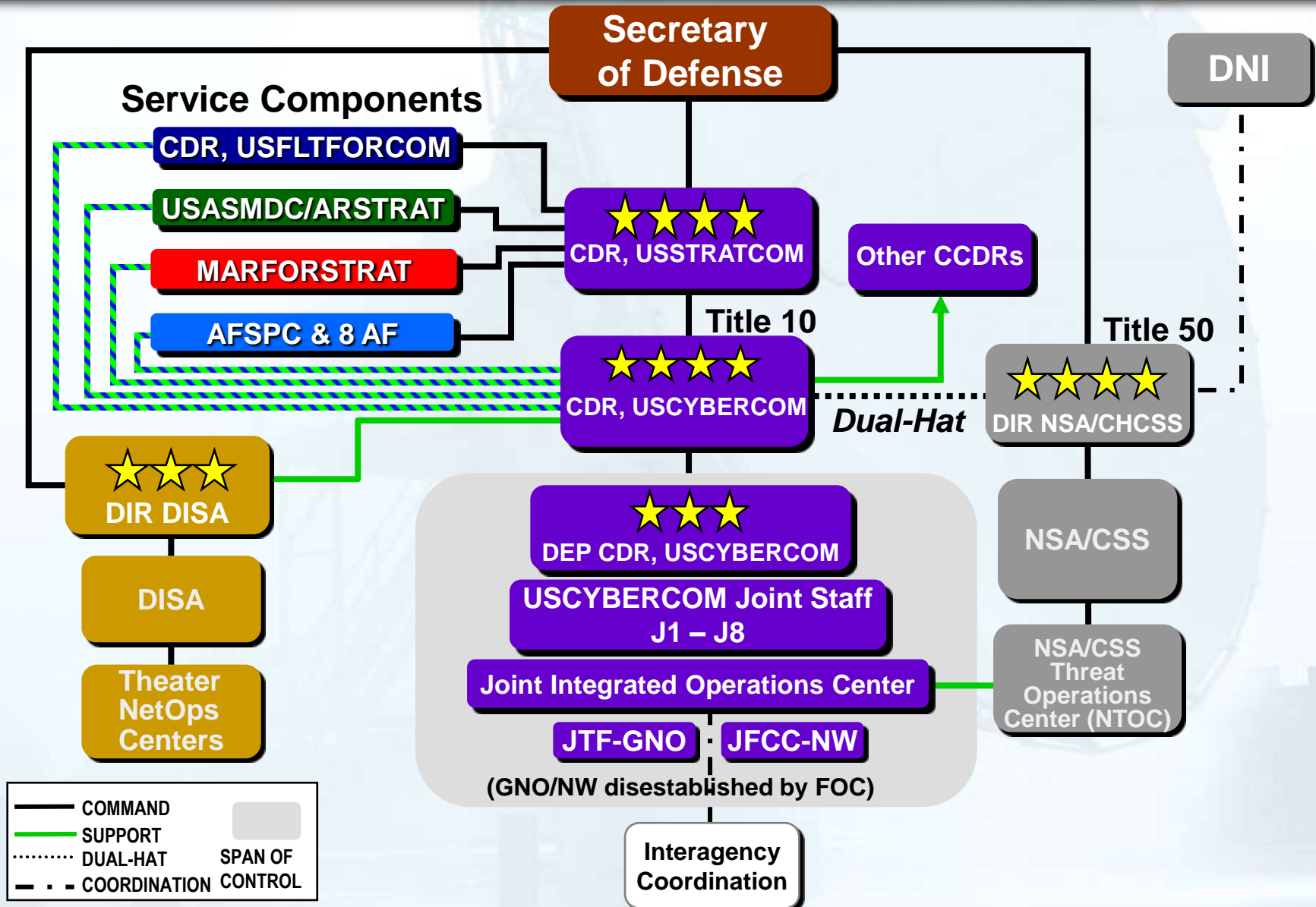
MOCS Action

Objective MOS Structure FY12





USCYBERCOM Organization

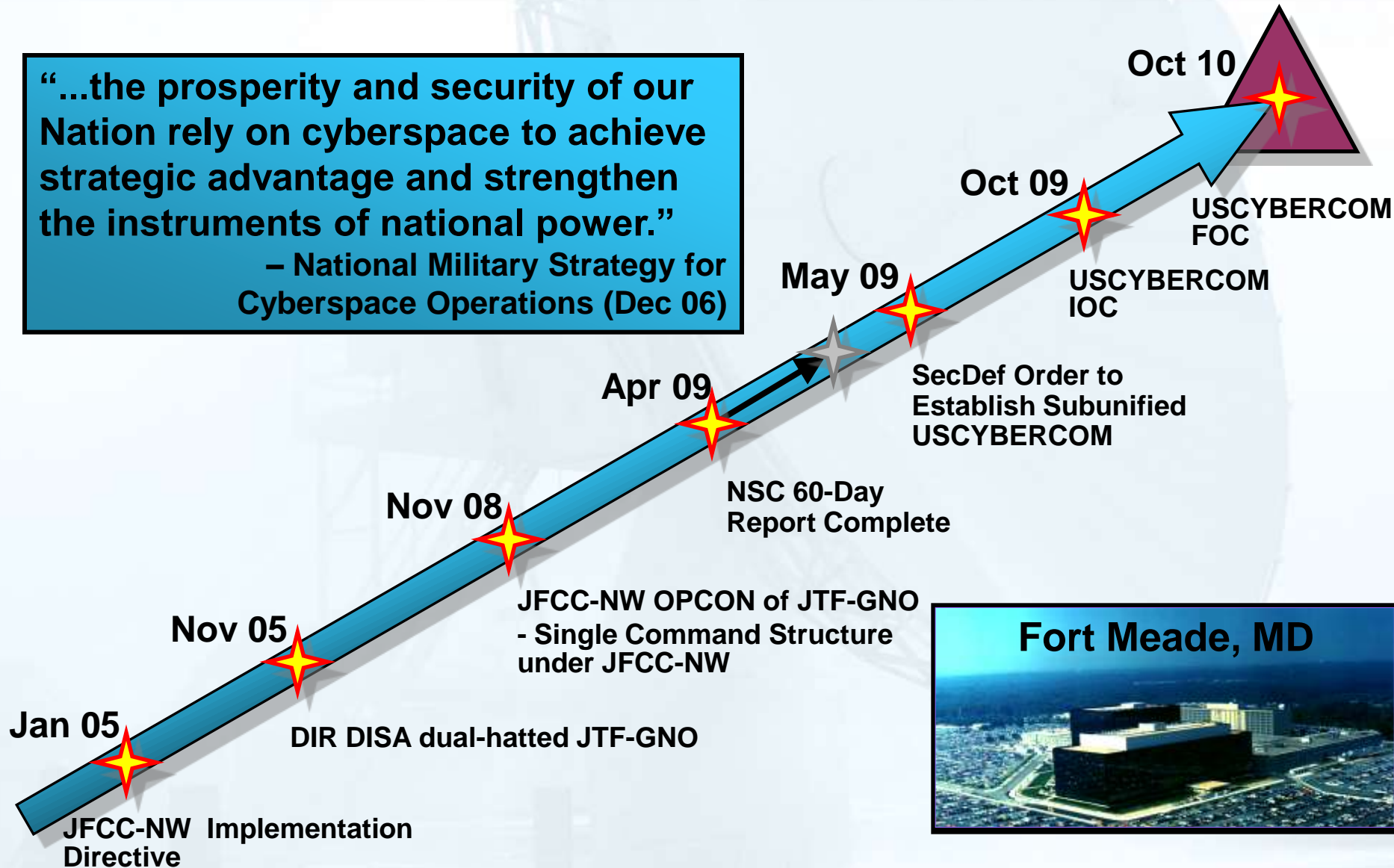




USCYBERCOM FOC Timeline



“...the prosperity and security of our Nation rely on cyberspace to achieve strategic advantage and strengthen the instruments of national power.”
– National Military Strategy for Cyberspace Operations (Dec 06)





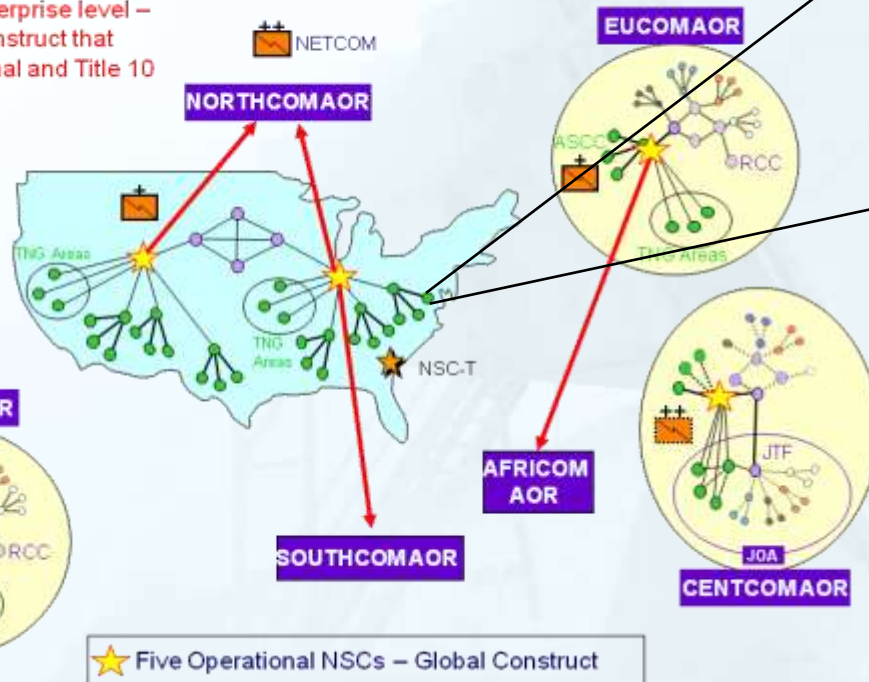
CONUS Installations In Global Context



- Extends the Army's global network construct to CONUS installations and beyond to network end devices
- Empowers a single Army command (NETCOM) to provide, operate, manage and defend the Army's global network
- Enables enterprise capabilities of Network Service Centers

Global Network Enterprise Construct

A single Army enterprise level – organizational construct that enables operational and Title 10 activities.



One Army Network – One Army Global Network Command



End-State Summary



➤ **NETCOM**

- Controls the global network & provides enterprise capabilities
- Responsible for Information Assurance/Computer Network Defense, configuration & management of devices on the network
- Required resources are assigned to NETCOM (IMCOM DOIMs)

➤ **Installations**

- No longer responsible for network & related functions on installation
- Retain responsibility for multi-media & visual information services (realigned to other garrison functions)

➤ **Tenants / Organizations / Units (including Garrisons)**

- Responsible for end-user device procurement, accountability & replacement
- Leaders remain responsible for enforcing policies & procedures

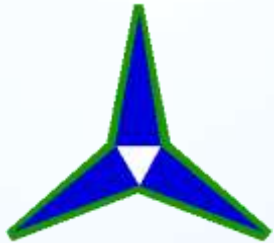


Army Warfighters' Forum (WfF)



I (US) Corps:

- Stryker Brigade Combat Team (SBCT)



III (US) Corps:

- Heavy Brigade Combat Team (HBCT)



XVIII Abn (US) Corps:

- Infantry (Light) Brigade Combat Team (IBCT)



Combined Arms Sustainment Command:

- Sustain Forum

... Other

Army WfF





WfF Website URLs



➤ **Stryker BCT WfF:**

<https://strykernet.army.mil/sites/warrior/default.aspx>

➤ **Heavy BCT WfF (Behind AKO):**

<https://www.us.army.mil/suite/page/432229>

➤ **Infantry BCT WfF (behind BCKS)** Can only be reached by clicking on *IBCT WfF link on ACOM home page on AKO*.
ACOM Portal Home Page:

<https://www.us.army.mil/suite/page/452027>

➤ **Sustainment WfF (Behind AKO):**

<https://www.us.army.mil/suite/page/372426>

Balancing Iraq & Afghanistan

Iraq

- **C4 Infrastructure**
 - Build Out Strategic Overwatch Bases (SOB)
 - Leverage Commercial Capabilities
- **C4 Forces**
 - Enable Future Operations



Afghanistan

- **C4 Infrastructure**
 - Build Out FOBs
 - Leverage Commercial Capabilities
- **C4 Forces**
 - Fix Baseline
 - Enable Future Operations
- **Define and Operationalize Mission Network**
- **Cross border communications**

Build operational flexibility in Afghanistan while preserving in Iraq

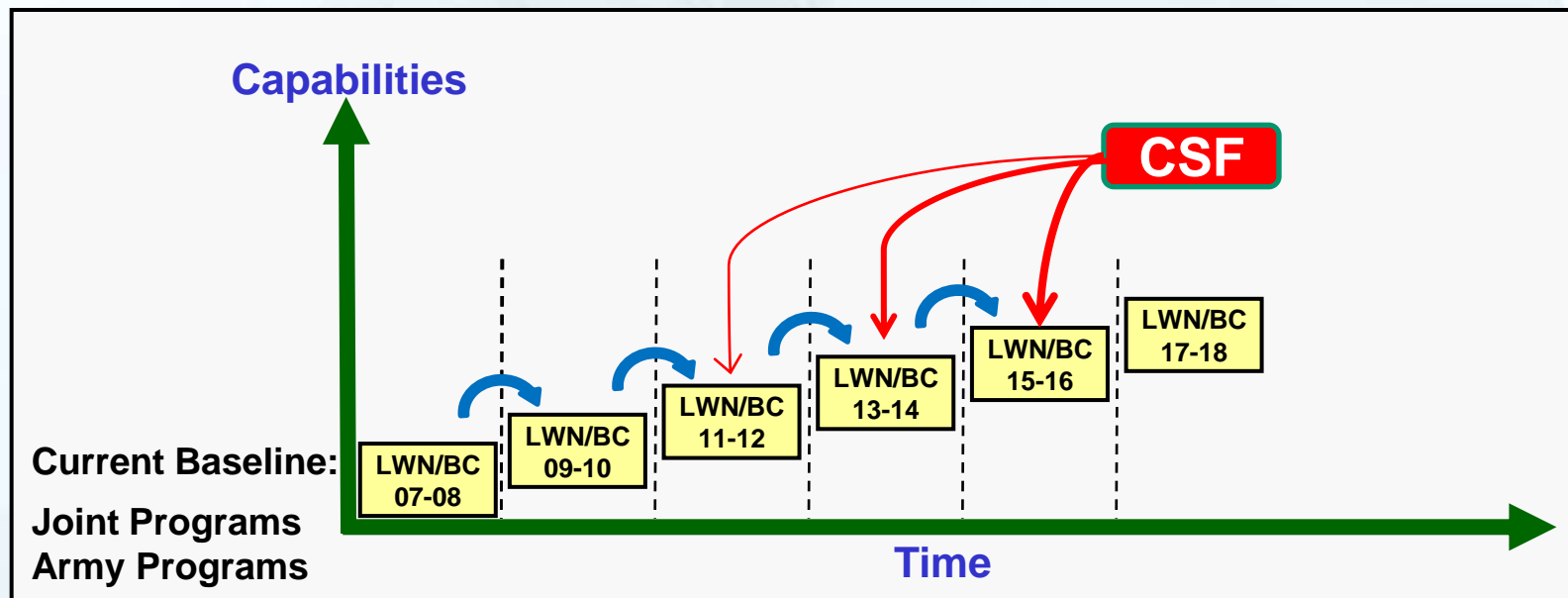


LWN/BC Strategy Framework



Objective: Deliver relevant, affordable, and interoperable LandWarNet/Battle Command capabilities sets to the Generating and Operational Force within the ARFORGEN process – over time

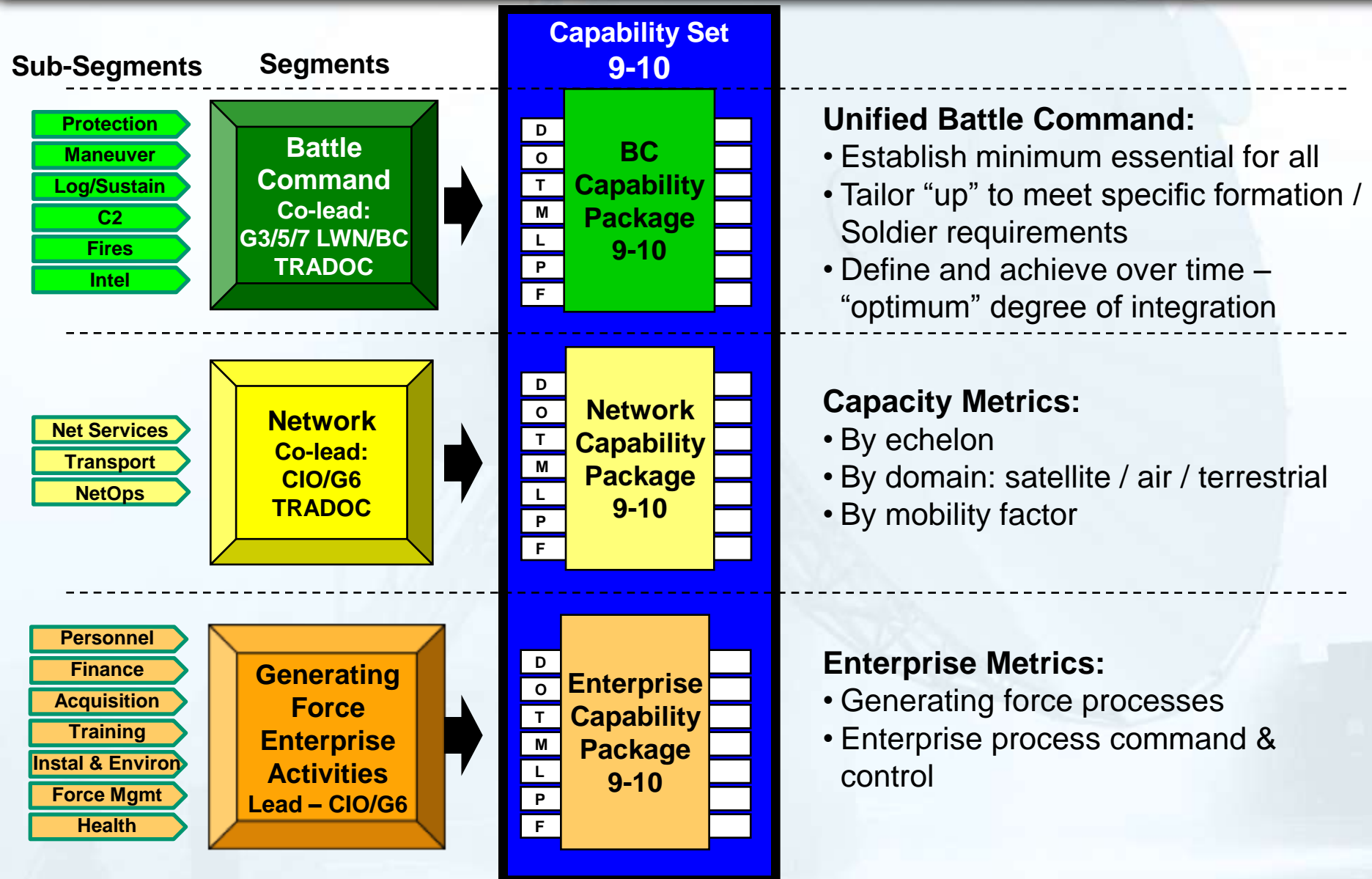
Framework: A portfolio construct focused on the development of Capability Sets for modular formations to synchronize and integrate all generating force processes to incrementally deliver improved capabilities – or modernize over time



All LWN/BC capabilities – in 2 year sets → tailored for each modular formation



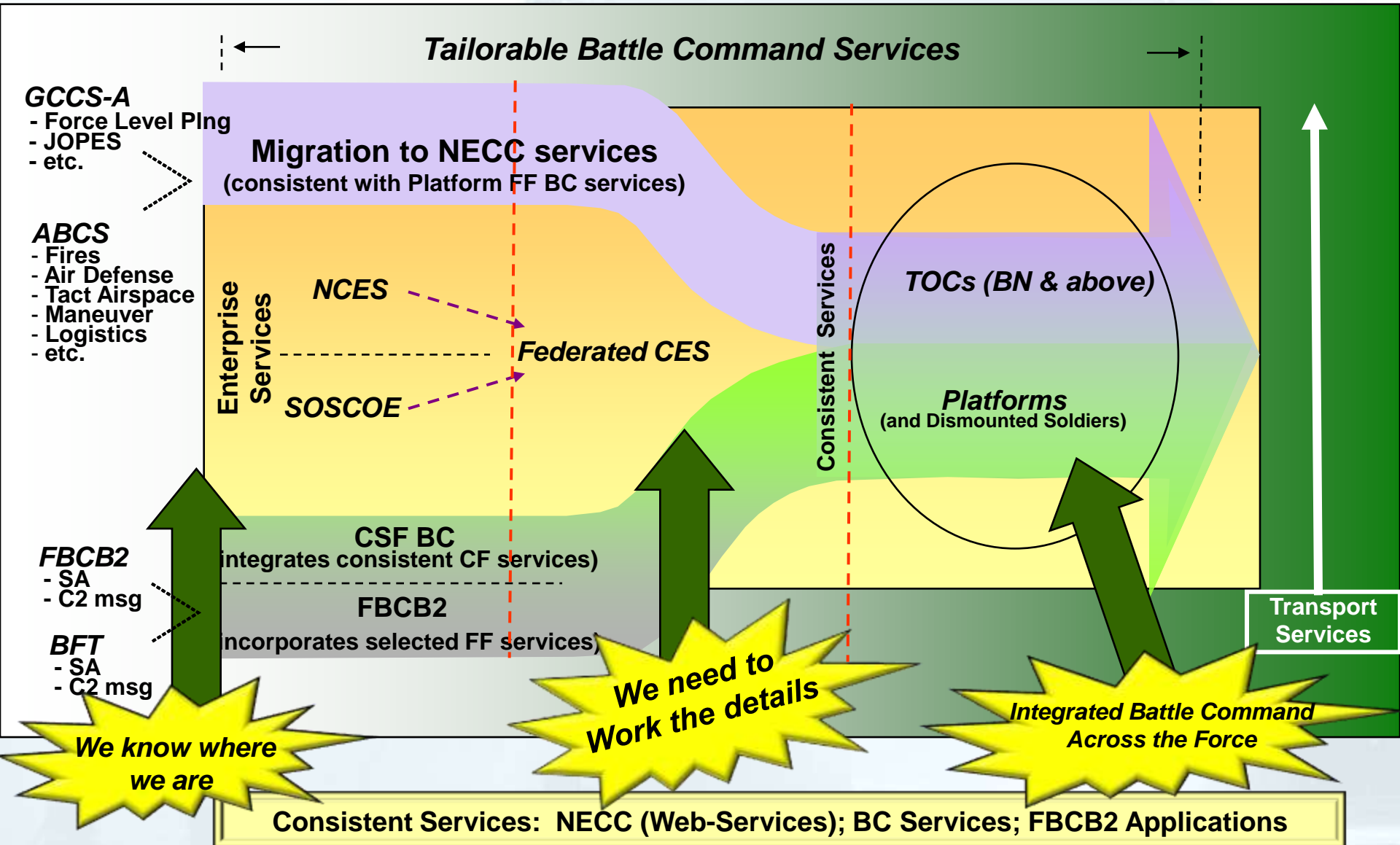
Capability Set – Portfolio Framework





Unified Battle Command

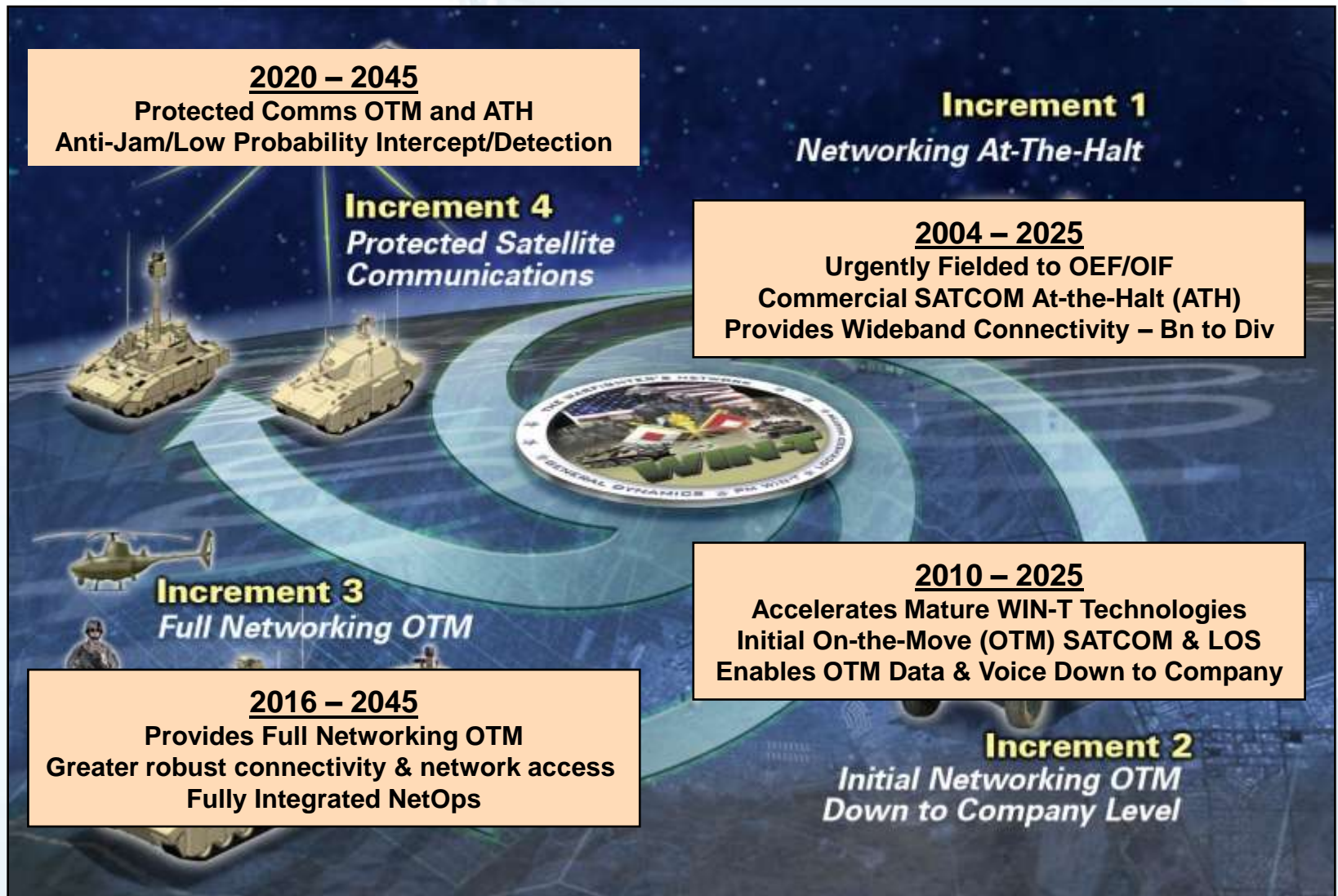
Consistent services supporting alternative Network environments





WIN-T Increments

DAE Certified / Restructured 5 June 07 ADM





WIN-T Increment 2

Proven Success in Dec 08



- **WIN-T INC 2 NetOps demonstration was highly successful**
 - ◆ NetOps Tools successfully planned and managed largest and most complex INC 2 network assembled to date (50 nodes) consisting of both OTM & ATH WIN-T systems utilizing one channel
 - ◆ Validated implementation of self-forming/self-healing network capability: resynchronized without human intervention
- **WIN-T OTM Radios (LOS & BLOS) met expectations and demonstrated TRL-6 and higher**
 - ◆ Excellent HNW & NCW connectivity, message completion rate is ~90%
 - ◆ NCW OTM demonstrated 256 Kbps – 2 Mbps
 - ◆ HNR OTM demonstrated 5 Mbps – 40 Mbps





TSAT Termination – Army Impacts



- **TSAT** was the centerpiece of the ***Transformational Communications Architecture*** (TCA)
- Recommendation to terminate TSAT creates capability gaps in:
 - ◆ **Capacity**: 54% of ground combatants in OA-08 scenario on TSAT – Must now move to WGS
 - ◆ **Throughput**: TSAT optimized for high capacity (T1), networked, protected signal to highly mobile users, WGS capable of 256 kbps – Current AEHF does not provide a ground force, high capacity COTM solution
 - ◆ **Terminal Density**: TSAT sized to reach thousands of mobile ground combatants – WGS will serve fewer users in an AOR
 - ◆ **Protection**: TSAT designed to provide AJ/AS service – WGS is subject to jamming disruption
- Recently completed TSAT Interim Design Review reveals several technologies that may have potential for WGS or AEHF upgrades

All Army SATCOM Stakeholders will work with AFSPC & Joint Community to achieve workable solutions



Conclusions



Army Imperatives

...working to restore balance to the Army



Global Network Enterprise Construct

...Way Ahead to support an Expeditionary Army



Cyber Operations

...organizing to focus efforts and support Joint Command



Space & C4

*...continuing to work with Joint Community
to achieve solutions for the Warfighter*





Service-Disabled Vet-Owned Small Business (SDVOSB) Opportunities



- Veterans Benefits Act of 2003 & Executive Order 13360 sets goal of 3% for SDVOSB Contracts
- Over 12,000 SDVOSB firms registered in Central Contractor Registration (CCR) Database
- Center for Veterans Enterprise maintain VetBiz Vendor Info Pages (VIP) Database
- Army Small Business Website useful resource for SDVOSB
<http://www.sellingtoarmy.info>
- Government Services Agencies Website useful resource as well
<http://www.gsa.gov/portal>



2009: ARMY YEAR OF THE NCO

Honoring and celebrating the
Army's Professional NCO Corps
tradition, and honoring NCOs
and their families for their
service and sacrifices!!



ARMY STRONG!

QUESTIONS + THOUGHTS



LTC Jeff Sorenson

Chief Information Officer/G-6

**AMERICA'S ARMY: THE STRENGTH OF THE NATION
ARMY STRONG**